SecurEnvoy

*White Paper*

# The risks of authenticating with digital certificates exposed

## Table of contents


Introduction ..... 2
What is remote access? ..... 2
Authentication with client side digital certificates ..... 2
Asymmetric encryption ..... 3
Issuance ..... 3
Life Cycle Management ..... 3
Handling Lost Devices ..... 4
The danger with distributed identities ..... 4
Combine rather than certify ..... 5
Doubly secure changes of device ..... 5
An overview of the advantages of tokenless 2FA ..... 6
Summary ..... 6

## Introduction

Change is the only constant in life - this quote from Heraclitus is just as relevant today as it was in ancient times. The world of work in particular has changed in recent years, first as a result of the use of desktop computers, then because of mobile devices such as laptops and mobile phones. Smartphones have evolved to become the "office in the jacket pocket", and the availability of mobile internet allows users to check e-mails and surf the web from almost anywhere. As a result, the traditional place of work has increasingly moved from the office building to other locations, such as home offices, cafés, hotel rooms and airport lounges. Digital certificates (cert) failed to take off in the late 1990's for end user authentication yet a decade on and the same issues still plague the adoption of certs it's just the wide spread stores of these failures have been forgotten.

This white paper explains how certificates work and explores common issues associated with them and compares them to tokenless two-factor authentication, which can be used as an alternative.

## What is remote access?

Remote access firmly established itself as a common term with the advent of the BYOD (Bring Your Own Device) trend, which refers to carrying out business activities using private, personal mobile devices. Remote access involves employees using a desktop computer, laptop, tablet PC or smartphone to access another computer, a corporate network or other internal communication facilities at another location via a dial-up connection or the Internet. The connection is established via the Remote Access Service (RAS) application service and its protocols, such as IPSec (Internet Protocol Security) and SSL (Secure Sockets Layer). However, before access is granted, employees must usually first authenticate themselves and prove that they have the necessary access rights and that they really are who they claim to be.

## Authentication with client side digital certificates

One possible solution for authenticating users is the use of a digital certificate. This is an identity certificate (basically a digital ID) that assigns a digital identity to a person. These certs can be used to confirm the authenticity of a user connecting to a web sites or remote access server. The key to trusting this cert is storing the

private key in a smartcard or portable device carried by the user. Certs consist of a data record that contains:

- the registered name of the certificate owner,
- the public key of the certificate owner,
- the date of issue and expiry date of the digital certificate,
- the registered name of the certification authority and
- the digital signature of the certification authority.

Cryptographic procedures are used to check the authenticity of certificates. Once a certificate has expired, it can no longer be used and must be replaced.

## Asymmetric encryption

Two encryption keys are used with certs: one private and one public. This is known as asymmetric encryption, because data is encrypted with a single key but decryption, however, requires a key pair consisting of a public and a private key. The private key is kept in a safe place by the user, who provides the public key to all third parties with whom data is exchanged.

## Issuance

The creation of digital certificates is handled by certification authorities (CA). These can be created internally in the organisation or companies can use the services of a commercial CA. When a user first enrols for a cert they must prove they are who they say they are. This can be done manually by checking personal documents such as passports or personal records which are very time consuming. Alternatively this process can be automated by leveraging tokenless two factor authentication via SMS to prove the users identity. After authentication the user's local device creates a key pair and passes the public key to the CA where it is signed by the CA's root key along with information about the user, the CA and the expiry date (typically 1 year). It is very important that the private key is stored within a secure area of the device (a virtual smartcard) so it can't be copied by malware software. Most CA's don't know how the private key will be stored so additional checking must be carried out before submission to the CA as to how the private key will be secured.

## Life Cycle Management

So what happens when the user's certificate expires after one year? They will no longer be able to authenticate with this cert and cannot use any remote access

services. They must re-enrol for a new certificate which will require them to again prove they are who they say they are. The user will need to log a support call to your helpdesk to request a new certificate or to be guided thought the process of re-enrolling if automated with tokenless two factor authentication.

What about the CA's certificate? All certificates including the CA's own self signed certificate have an expiry date which in the case of a CA is typically 5 years. When this expires, all certificates issues by this CA will no longer be valid! Thousands of users will simultaneously stop working and all users must re-enrol with the new CA certificate!

## Handling Lost Devices

Backend VPN or web servers must check the validity of a cert by submitting an online query via OCSP (online certificate status protocol). The request goes to an OCSP server, which provides information about the status of the cert in terms of it being "good", "blocked" or "unknown". The answers come from the CA that keeps a record of the status of the cert, this addition check may also cause delays in the login process OCSP supplements or replaces the more widely used Certificate Revocation List (CRL). This list must be completely downloaded and is typically stored locally for 24 hours. A CRL contains all the serial numbers of the currently invalid certs that are either blocked (temporarily not available) or revoked (i.e. permanently unusable). Because CRL's are only downloaded periodically there is less delay getting cert status after the initial download however lost devices can still be used for up to 24 hours after reporting them missing!

## The danger with distributed identities

There is also a danger associated with distributed identities. With the advent of BYOD more and more users wish to use their portable phones and tables device. Given that it is not practical to support an external smartcard with these devices, each device will require its own digital certificate and thus will require a separate enrolment request. The more devices a user works with, the more he/she scatters his/her digital identity around.

So what happens when the device is replaced with a new one? Typically the private key will be stored in a "virtual smartcard" which is part of the hardware of the device

so the new device will require enrolling from scratch. Such an approach will quickly lead to even more scattering of a user's identity, consideration of how to check that old devices will be correctly revoked when no longer required is important.

## Combine rather than certify

A more secure method is provided by two-factor authentication (2FA), as it is personal and combines two components, with a login only being permitted upon entry of the correct combination. With this approach, at least two of three factors are required in order to clearly identify a user:

- something known only to the user (e.g. PIN);
- something they own (e.g. keys, credit card or their mobile phone) and/or
- something that is unique to the user, such as a finger print.

This principle is familiar from, for example, the withdrawing of money from an ATM: in order to carry out a successful transaction, the customer needs both a personal bank card and a PIN. Access to the account remains blocked if either of these two components is missing or if the PIN is not entered correctly. The user can select one of his/her devices (something they own) to act as their tokenless authenticator - for example their mobile phone, and use this device to authenticate to all other devices, PC's, laptops, cyber-cafés or business lounge login's without leaving their identity spread everywhere.

## Doubly secure changes of device

The life cycle management of the chosen devices is also furnished with specific security measures. This ensures that only one device can be used for authentication at any one time. If a user switches, for example, from his/her smartphone to a tablet, this device now becomes their authentication token for use with all other devices whether they are owned, shared or publicly used. Any OTPs that remain on the smartphone are automatically deleted on the backend server. An upgrade to another newer model works in the same way: the user uses his/her previous mobile device in order to authenticate himself/herself to provision the new one. The system then automatically deletes the seed record on the server associated with the old device. Thus there is no longer any risk involved in leaving identities or older devices that may later become sold.

SecurAccess also increases the level of security by dividing the seed records, which are special algorithms used to create the one-time passcodes. Part of the record is generated locally within the server and passed to the device via a QR code, while the second part is defined using characteristic properties of the mobile device used. This effectively forms a "finger print" consisting of information such as the CPU serial number or equivalent. Each time the user requests a passcode, the user's device decrypts the first part of the seed record and derives the second part accordingly, thus only part of the seed record is ever stored on the device.

## An overview of the advantages of tokenless 2FA

- The user can nominate one device and use it like a hardware token to login on any other device
- No splattering of identity on multiple devices
- No periodic re-enrolment is required
- No mass outage when CA expires
- No certificate checking delays
- No 24 hour risk period as 2FA can be disabled in real time
- There is no need for additional hardware tokens, which have to be purchased, configured, maintained and regularly replaced if lost or stolen
- It works with all the latest mobile phones, smartphones, laptops, tablets, Microsoft PCs and Apple Macs

## Summary

Certs failed to take off in the late 1990's for end user authentication yet a decade on and the same issues still plague the adoption of certs it's just the wide spread stores of these failures have been forgotten. They are not mature enough to provide client side authentication. The technology has evolved in the direction of 2FA. With this, companies can ensure that their staff are unambiguously identified, as only the correct combination of user details and an OTP permits a successful login on any device owned or shared. The use of tokenless 2FA software is also associated with other advantages, such as cost savings and easy deployment. In addition, employees can simply use their existing mobile devices that they generally carry around with them anyway. And in terms of life cycle management they can upgrade their phone without logging a support call or leaving their identity on their previous device, split seed records ensure greater security as a result of the regulated use of

only one device that acts as the “hardware token” which is then used to authenticate all other logins on any other device including its self.